UNIVERSIDAD ICESI
Calle 18 No. 122-125, Cali. Colombia
PBX (57-2) 555 2334, Fax (57-2) 555 2334
www.icesi.edu.co

TALLER PRÁCTICO

DESARROLLO BACKEND

Objetivo

Con este ejercicio, los participantes podrán practicar el manejo de autenticación y autorización en una aplicación Spring Boot con una capa de datos sencilla. También aprenderán cómo crear endpoints para el registro de usuarios, el inicio de sesión y la gestión de usuarios registrados, y cómo crear una clase Repository para manejar los datos de la aplicación de forma local.

Enunciado

En este taller práctico, crearemos una aplicación Spring Boot con una capa de datos sencilla para el registro de usuarios y su autenticación. Los participantes del taller deberán crear los siguientes endpoints:

1. Endpoint para el registro de usuarios: Este endpoint debe permitir a los usuarios registrarse y crear un objeto de usuario con un UUID único.

2. Endpoint para el login: Este endpoint debe permitir a los usuarios autenticarse y recibir su objeto de usuario como respuesta. El UUID recibido en la respuesta debe usarse como valor de la cabecera "Authentication" para usar los dos siguientes endpoints.

3. Endpoint para listar usuarios: Este endpoint debe permitir a los usuarios autenticados listar todos los usuarios registrados. La autenticación se realiza a través de la cabecera "Authorization", que debe contener el UUID del usuario registrado. La validación de que el usuario está registrado debe hacerse antes de ofrecer la lista de usuarios.

4. Endpoint para editar usuario: Este endpoint debe permitir a los usuarios autenticados editar su propia información de usuario. Para acceder a este endpoint, también se requiere la cabecera "Authorization".

5. Endpoint para eliminar usuario: Este endpoint debe permitir a los usuarios autenticados eliminar su propia cuenta. Para acceder a este endpoint, también se requiere la cabecera "Authorization".

Es importante destacar que los participantes deberán crear una clase *Repository* para manejar el registro de usuarios y su autenticación. Esta clase tiene como objetivo actuar como una capa intermedia entre los datos y la lógica de negocio de la aplicación. En este caso, la clase Repository se encargará de manejar el registro de usuarios y su autenticación sin la necesidad de conectarse a una base de datos.

UNIVERSIDAD ICESI
Calle 18 No. 122-125, Cali. Colombia
PBX (57-2) 555 2334, Fax (57-2) 555 2334
www.icesi.edu.co

La clase Repository debe contener métodos para la creación, actualización y eliminación de usuarios, así como para la autenticación de usuarios registrados.

Códigos de respuesta HTTP

Para cada uno de los endpoints responda adecuadamente para las posibles respuestas que otorga cada endpoint.

1. Registro de usuarios:
   - 201. (Created): El usuario ha sido creado correctamente.
   - 400. (Bad Request): Si la solicitud contiene un formato o datos incorrectos.
   - 409. (Conflict): Si el usuario ya existe en la base de datos.

2. Login:
   - 200 (OK): Si la autenticación es exitosa y se devuelve el objeto de usuario correspondiente.
   - 401 (Unauthorized): Si la autenticación falla, es decir, las credenciales proporcionadas son incorrectas.

3. Listar usuarios:
   - 200 (OK): Si la solicitud se realiza correctamente y se devuelve una lista de usuarios.
   - 401 (Unauthorized): Si el usuario no está autenticado o las credenciales proporcionadas son incorrectas.

4. Editar usuario:
   - 200 (OK): Si la solicitud de actualización se realiza correctamente.
   - 401 (Unauthorized): Si el usuario no está autenticado o las credenciales proporcionadas son incorrectas.

5. Eliminar usuario:
   - 200 (OK): Si la solicitud de eliminación se realiza correctamente. Devuleva el objeto de usuario eliminado.
   - 401 (Unauthorized): Si el usuario no está autenticado o las credenciales proporcionadas son incorrectas.